

Dissenting Views to Accompany H.R. 5825, the “Electronic Surveillance Modernization Act

We strongly support intercepting each and every conversation involving al Qaeda and its supporters. We have in the past and continue to support common sense updates to the Foreign Intelligence Surveillance Act (“FISA”) so that our surveillance capabilities can keep pace with modern technologies – as a matter of fact, all of us supported a bipartisan substitute offered by Reps. Schiff (D-CA) and Flake (R-AZ) which would have accomplished these goals without sacrificing our rights and liberties.¹ However, we dissent from the legislation reported by the Judiciary Committee because instead of bringing the President’s warrantless surveillance program under the law, it dramatically expands his authority and permits even broader and more intrusive warrantless surveillance of the phone calls and emails of innocent Americans. The legislation also raises severe constitutional questions, and was subject to an ill-considered and unfair process.²

Description of the Legislation

The legislation reported by the Committee proposes numerous significant changes to FISA, which governs the surveillance of foreign powers, terrorist organizations and their agents. These changes would dramatically expand the ability of the Administration to wiretap and gather information on innocent Americans without court approval or legal recourse.

The legislation amends FISA in several ways that would expand the Administration’s ability to eavesdrop on telephone calls, e-mails and other communications of U.S. citizens, without obtaining court approval. First, Section 3(b) alters the definition of “electronic surveillance” in a manner that permits the warrantless surveillance of the international communications of any American who is not a specific target.³ The bill also amends an

¹The Majority rejected this bipartisan substitute amendment by a vote of 18-20. The bipartisan amendment included language: (1) clarifying the Authorization for Use of Military Force did not contain legal authority for warrantless wiretapping in the United States; (2) reiterating that FISA is the exclusive means of conducting electronic surveillance for foreign intelligence in the United States; (3) requiring the President must submit a report to Congress on classified surveillance programs; (4) permitting the Chief Justice of the United States can appoint additional FISA judges; (5) streamlining the FISA application process; (6) extending emergency FISA authority from 3 days to 7 days; (7) allowing for use of wartime FISA exception also after congressional authorization for use of military force; (8) clarifying that FISA warrants are not needed for intercepting foreign-foreign communications; and (9) authorizing the hiring of additional intelligence personnel.

²The legislation is opposed by technology companies and groups concerned with the civil liberties of Americans, including the Computer & Communications Ind. Ass’n, the ACLU, the Center for National Security Studies, and the Center for Democracy and Technology.

³Section 3(b) of the reported bill proposes a number of changes to FISA, one of which amends the definition of “electronic surveillance” in FISA to the (1) interception of

operative section of FISA to permit warrantless surveillance of Americans for one year if it involves communications with foreign powers. Proposed new section 102 of FISA (added by section 4 of the bill) accomplishes this by eliminating a requirement in current law requiring that when the government wiretaps foreign powers, there should be no substantial likelihood that Americans' conversations will be captured.⁴

Proposed new section 102A of FISA also grants the Administration new unilateral authority to conduct any and all forms of allegedly non-wiretap surveillance on innocent U.S. citizens so long as one of the targets is "reasonably believed to be outside of the United States." This section, for example, would permit the Administration to review call records and other stored communications from communication providers and other persons and perhaps even content if the Attorney General merely certifies the information is not electronic surveillance as defined in FISA.⁵

Under proposed new section 102B of FISA, the Attorney General would be granted the unilateral power to implement the new intelligence authorities identified in new sections 102 and 102A by demanding that any person – including a communications provider, internet company, landlord, or family member – assist with the execution of both electronic surveillance or other acquisition of intelligence information (such parties would also be insulated from legal liability for complying with such a directive). Any individual challenging the directive would have limited rights to challenge the order in court.⁶

The bill also permits the government to permanently retain surveillance information

communications acquired by targeting a person who is reasonably believed to be in the United States; and (2) interception of any communication if both the sender and all recipients are in the United States.

⁴Section 4(a) of the bill proposes a new section 102 of FISA that would allow the surveillance without a court order of communications of foreign powers but would *not* contain an exclusivity limitation that exists in current law; as a result, it would apply to all six categories of foreign powers and could permit capture of communications to or from U.S. persons.

Section 4(a) of the bill also proposes a new section 102A of FISA that would allow the government to acquire intelligence information about persons the government asserts are not in the United States. In such cases, the Attorney General could obtain an order for up to one year without a court order if the acquisition does not constitute electronic surveillance but pertains to foreign intelligence information.

⁵For instance, the Attorney General could say that surveilling communications from inside the United States to outside the United States does not constitute "electronic surveillance" within the definition of FISA. As such, he may argue that the government does not require a warrant and could collect as much content as desired and without limitation.

⁶This cause of action likely is pre-empted by section 11 of the bill, which prohibits any court review of any actions related to any intelligence programs.

inadvertently collected on innocent Americans pursuant to these and other provisions of FISA.⁷ Section 4 of the bill does this by rewriting provisions in existing law that govern the use of information collected pursuant to FISA directives under new section 102B to strike an existing requirement that unintentionally-acquired information be destroyed unless there is a threat of death or serious injury.⁸ Section 8 of the bill further permits the government to retain permanently any unintentionally-acquired information collected pursuant to wire, radio, or electronic communications if the government finds foreign intelligence information is present (current law is limited to the retention of radio communications if there is information about a death or serious bodily injury).

In addition and significantly, the bill would eliminate court review of intelligence programs. Section 11 of the bill (incorporating the amendment offered by Rep. Chris Cannon (R-UT)) would preclude any court from hearing any case or imposing any civil or criminal liability over any activity related to any “alleged intelligence program involving electronic surveillance” that is certified by the Attorney General to be intended to protect the United States from a terrorist attack. In addition to having the effect of dismissing all pending challenges to the legality of the president’s warrantless surveillance program, this provision would prevent any other legal challenges from being brought in the future concerning any misuse or abuse of surveillance powers.

The legislation contains other provisions that expand Administration power to obtain information, including:

- Section 3(a) of the legislation, which broadens the government’s ability to obtain information from foreign persons located within the United States, including individuals and corporations, even if they have no connection to a foreign government or terrorist organization.⁹

⁷See new section 102B of FISA as proposed by the reported bill.

⁸Section 106 of FISA (section 1806 of title 50) governs the use of information collected via FISA.

⁹Section 3(a) of the bill would add to the category of non-U.S. persons who could be agents of foreign powers. It would include anyone (including corporations) who “is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the official making the certification [for a FISA order] deems such foreign intelligence information to be significant.” Current law defines “foreign intelligence information” as (1) that which can protect the United States against terrorist attack or (2) information with respect to a foreign power or territory that relates to the defense or security or foreign affairs of the United States. 50 U.S.C. § 1801(e).

Under the new definition, it is possible that the foreign employee of a U.S. corporation could be subject to a wiretap if his or her job entails working with encryption technology or computer parts (either of which could constitute foreign intelligence information).

- Section 6 of the bill, which permits any official designed by the President, even those involved in leaking classified information, to seek FISA surveillance requests. Currently, only the National Security Adviser or Senate-confirmed presidential appointees with responsibility for national security or defense can submit a certification in a FISA application that the wiretap is needed to collect intelligence.¹⁰
- Section 7 of the legislation, which makes it more difficult for judges to review extensions of FISA orders. Under the legislation extensions of FISA orders would have to be issued for periods of up to one year; the current limit is 90 days in most cases.
- Section 7 of the legislation also eliminates the requirement that the government obtain a court order prior to installing a pen register or trap-and-trace device. The bill does this by providing that anytime a judge issues an order for electronic surveillance involving communications the judge also must issue an order authorizing the use of pen register and trap-and-trace devices related to such communications.
- Section 7 permits any Senate-confirmed presidential appointee to authorize emergency surveillance, even those that have nothing to do with national security or the Justice Department. Congress recently amended FISA to permit the Deputy Attorney General or the Assistant Attorney General for National Security to make such emergency authorizations.¹¹

The bill also includes a few provisions nominally designed to rein in surveillance abuses, but which appear in actuality to be mere “window dressing.” For example, section 12 of the bill contains a provision requiring the Director of the National Security Agency, in consultation with the Director of National Intelligence and the Attorney General, to submit to the House and Senate intelligence committees a report on minimization procedures.¹² In addition, section 2 of the bill includes a “finding” that the necessary and proper clause of the Constitution grants Congress the authority to regulate the President’s power to gather foreign intelligence.¹³ This is a non-binding assertion, and given the President’s proclivity to interpret laws that fly in the face of

¹⁰The legislation also broadens the government’s authority with respect to emergency FISA surveillance, instances when the government can use FISA surveillance absent a court order. In addition to extending from 3 days to 7 days the period permitted for emergency surveillance, it also would permit any Senate-confirmed presidential appointee to authorize emergency surveillance; current law limits that authority to Justice Department officials: the Attorney General, Deputy Attorney General, the Assistant Attorney General for National Security.

¹¹ Sec. 506(a)(5) of Public Law 109-177.

¹²Section 12 of the reported bill. This report specifically would pertain to the applicability of such procedures to information concerning U.S. persons acquired under FISA electronic surveillance as it has been defined prior to the date of enactment of this bill.

¹³Section 2 of the reported bill.

supposedly-binding statutory language,¹⁴ cannot be expected to provide any meaningful limitation on the president's authority. Also, Section 9 states that reports on FISA use would go to all members of the intelligence committees (as opposed the committees as a whole as provided in current law). This modest step will do very little to enhance accountability.

Finally, the legislation includes a number of miscellaneous and less controversial provisions. For example, section 7 of the legislation extends from 3 days to 7 days the period permitted for emergency surveillance. Section 6 would permit the government to submit a summary of information supporting a FISA application as opposed to a complete description. Section 10 of the bill provides that if a FISA physical search or surveillance warrant is issued for a person in the United States, then that warrant would continue in effect if the person leaves the United States.

Concerns with the Legislation

A. The Legislation Contains Significant New Statutory Authorizations that Threaten the Privacy of Innocent Americans

An initial concern with the legislation is that it does not impose any limits on the President's power to conduct warrantless surveillance on innocent Americans in violation of FISA. This is because the bill does not state that it contains the exclusive means for the government to conduct surveillance, warrantless or otherwise.¹⁵ Rather, the legislation appears to assume the president has "inherent authority" to conduct the type of warrantless surveillance first disclosed by *The New York Times* in December, 2005, and goes beyond that to grant the president even further statutory authority to intercept the communications of innocent Americans without any court approval. The Justice Department even admitted as such when it testified before the Crime Subcommittee that the bill and the warrantless wiretapping program are separate.¹⁶

Second, the legislation permits vastly expanded government wiretapping of innocent Americans without a warrant and without probable cause. As described above, the bill allows for

¹⁴Charlie Savage, *Bush Challenges Hundreds of Laws: President Cites Powers of His Office*, BOSTON GLOBE, Apr. 30, 2006, at A1.

¹⁵The Majority rejected two efforts at ensuring that FISA would be the exclusive means of collecting foreign intelligence via electronic surveillance. The Majority first rejected by a vote of 18-20 a bipartisan amendment offered by Rep. Jeff Flake (R-AZ) and Rep. Adam Schiff (D-CA) that clarified that FISA was the exclusive means of conducting such surveillance. The Majority also defeated by voice vote an amendment offered by Rep. Sheila Jackson Lee (D-TX) clarifying such exclusivity.

¹⁶H.R. 5825, the "Electronic Surveillance Modernization Act," *Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 109th Cong., 2d Sess. (Sept. 12, 2006) (statement of John Eisenberg, Deputy Assistant Attorney General, Office of Legal Counsel, U.S. Dep't of Justice).

warrantless wiretapping of virtually all international communications, even if they involve a person within the United States, including U.S. citizens, as long as the government asserts that it was not targeting a U.S. citizen. As Jim Dempsey of the Center for Democracy and Technology testified, “[c]urrently, FISA requires a court order to intercept wire communications into or out of the [United States], many of which involve U.S. citizens. Under the proposed new [definitions in the bill], wire communications to or from the [United States] could be intercepted using the vacuum cleaner of the NSA, without a warrant, so long as the government is not targeting a known person in the [United States].”¹⁷ The Computer and Communications Industry Association – a trade association including Microsoft, Google, and Verizon – agreed, writing that “the mere possibility of widespread, secret, and unchecked surveillance of the billions of messages that flow among our customers, especially U.S. citizens, will corrode the fundamental openness and freedom necessary to our communications networks.”¹⁸ The Administration has never articulated why such vast new authority to conduct warrantless surveillance involving innocent Americans is necessary, given that FISA already permits surveillance to be conducted without a warrant on an emergency basis prior to obtaining court review.

Third, the legislation authorizes the Attorney General to unilaterally engage in non-electronic surveillance involving innocent Americans (such as reviewing stored communications and call records) and unilaterally issuing directives against communications providers to obtain both electronic surveillance and other information. We have never received any justification for such broad new and unchecked authority, which was slipped into the legislation at the last minute with no supporting record or adequate explanation.

Fourth, we are concerned that allowing the government to maintain permanent records on innocent U.S. citizens based on the records of their warrantless surveillance would also unnecessarily intrude on the privacy rights of innocent Americans. Under current law, the required destruction of unintentionally-acquired FISA information ensures that the government cannot maintain records on individuals, such as American citizens, who pose no threat to the nation. The bill would remove entirely any protections that U.S. citizens and lawful permanent residents have from government surveillance. These records could include information related to First Amendment and Second Amendment activity. Again, we have never received a justification for such expanded intrusions on American’s privacy.

Fifth, the legislation includes an unprecedented court stripping provision in the form of

¹⁷*Legislative Proposals to Update the Foreign Intelligence Surveillance Act (H.R. 4976, H.R. 5223, H.R. 5371, H.R. 5825, S. 2453, and S. 2455.): Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary, 109th Cong., 2d Sess. (Sept. 6, 2006).*

¹⁸Letter from Ed Black, President and CEO, Computer & Communications Ind. Ass’n, to the Hon. F. James Sensenbrenner, Jr., and the Hon. John Conyers, Jr., House Comm. on the Judiciary, Sept. 19, 2006. The Association further noted that this unchecked surveillance could lead to retaliation and similar communications surveillance on Americans by other countries. It wrote that its “industry is confronted with escalating monitoring and surveillance by repressive foreign regimes. When challenged, totalitarian states often justify their policies by pointing to U.S. government practices.” *Id.*

the Cannon Amendment which would not only terminate pending and future cases challenging the president's controversial warrantless surveillance program, but would nullify the few rights provided to American citizens in the legislation. For example, while the legislation grants persons the nominal right to challenge directives to provide intelligence information to the Attorney General, the Cannon amendment – which supercedes any and all inconsistent laws – strips the court of that authority.

Finally, we would dispute the proponents much repeated assertion that the committee-reported legislation is needed to “modernize” FISA and make it “technology neutral.” The Congressional Research Service has confirmed that since its inception in 1978, 51 separate provisions in twelve different laws have updated FISA, many of them made in the last five years.¹⁹ To the extent further changes are required, we all supported the provisions included in the Schiff-Flake substitute which eliminated the law's differential treatment of different technologies and approved warrantless surveillance of all foreign to foreign communications which transmit through the U.S.

B. The Legislation Raises Significant Constitutional Questions

The legislation raises serious if not intractable questions under both the Fourth Amendment and the principle of separation of powers and due process.

First, the bill may well violate the Fourth Amendment protections against “unreasonable searches and seizures,” and requiring judicially approved warrants issued with “particular[ity]” and “upon probable cause.” There is little doubt that the Fourth Amendment fully applies to electronic surveillance. In *Katz v. United States*,²⁰ the Supreme Court held that the Fourth Amendment requires adherence to judicial processes in the case of national security wiretaps, and that searches conducted outside the judicial process, are *per se* unreasonable under the Fourth Amendment, subject only to emergency and similar exceptions. In *United States v. U.S. District Court (the Keith case)*,²¹ the Court specifically held that, in the case of intelligence

¹⁹Since the September 11 attacks, Congress amended FISA to extend its emergency exemption from 24 to 72 hours, and the PATRIOT Act included some twenty-five separate updates to FISA including: (i) expanding the scope of FISA pen register authority; (ii) lowering the standard for FISA pen-traps; (iii) lowering the legal standard for FISA surveillance; (v) extending the duration of FISA warrants; (vi) expanding the scope of business records that can be sought with a FISA order; (vii) allowing for “John Doe” roving wiretaps; (viii) requiring the intelligence community to set FISA requirements and assist with dissemination of FISA Information; (ix) immunizing those complying with FISA orders; (x) lowering the standard for National Security Letters; and (xi) expanding NSL approval authorities. Subsequent to the passage of the PATRIOT Act, Congress has again at the Administration's request broadened FISA to allow surveillance of “Lone Wolf” terrorists and the FISA courts have streamlined their procedures to accommodate the Administration's requests.

²⁰389 U.S. 347 (1967).

²¹407 U.S. 297 (1972).

gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.²² As discussed above, the legislation permits the widespread practice of intercepting the international telephone calls and e-mails of innocent Americans. As such, it would seem to contradict the requirements of the Fourth Amendment, as long interpreted by the courts.

Second, the bill would seem to violate separation of powers and due process requirements.²³ It does so with respect to the Cannon amendment, which would preclude any court from hearing any legal challenges related to intelligence programs involving electronic surveillance. Despite the fact that Article III of the Constitution grants to the courts the judicial power over all cases in law and equity arising under the Constitution and laws of the United States, and harmed individuals have long been understood to be entitled to assert their due process rights in a court of law, the Cannon amendment would bar existing and future lawsuits and preclude any civil or criminal liability, including injunctive relief, for any activity related to any intelligence program involving FISA's definition of electronic surveillance.²⁴ Such immunity is retroactive to any program in existence dating back to September 11, 2001. As noted above, the practical impact of the Cannon amendment is to nullify the enforceability of any rights granted in the bill or otherwise to protect one's privacy. Kate Martin of the Center for National Security Studies notes the breadth of the Cannon amendment, observing, "the amendment ... would jeopardize Americans' fundamental right to challenge unconstitutional surveillance of their communications in court."

C. The Legislation was Considered under a Flawed and Unfair Process

The entire process by which this legislation traveled through the Judiciary Committee was seriously flawed. At the outset, attempts at conducting independent investigations of the President's program were thwarted at every turn. Nearly nine months after we first learned of the warrantless surveillance program, there has been no attempt to conduct an independent inquiry into its legality. Not only has Congress failed to conduct any sort of investigation, but the Administration summarily rejected all requests for special counsels as well as reviews by the

²²*Id.* at 313-14, 317, 319-20. The Court further stated: "These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillance may be conducted solely within the discretion of the Executive Branch." *Id.* at 317-318.

²³By denying the courts their historical role as the final legal authority, the legislation appears to usurp judicial power. Since the Supreme Court's ruling in *Marbury v. Madison*, the separation of powers doctrine has been well established. *See Marbury v. Madison*, 5 U.S. 137 (1803).

²⁴It is important to note that the Majority rejected by a vote of 14-22 an amendment offered by Rep. Jerrold Nadler (D-NY) to preserve the ability of courts to order injunctive relief for unlawful government programs.

Department of Justice and Department of Defense Inspectors General.²⁵ When the Justice Department's Office of Professional Responsibility finally opened an investigation, the President himself squashed it by denying the investigators security clearances.²⁶ Furthermore, the Department has completely ignored the numerous questions posed by this Committee and the Wexler Resolution of Inquiry the Judiciary Committee previously adopted requesting copies of Administration documents concerning surveillance activities.²⁷

Second, Members of the Committee have never been briefed on the nature and extent of the President's warrantless surveillance program. Although, the Justice Department did conduct a briefing for House Judiciary Committee Members on September 12, 2006, that briefing was limited to the tech neutrality portion of the Wilson bill. The NSA failed to honor or even respond to a request made by sixteen Democratic Members of the Judiciary Committee for even a classified briefing on the entirety of the NSA program.²⁸

Third, the process by which the markup was conducted was both haphazard and unfair, as the Majority substantially altered the bill without providing Minority Members any notice or opportunity to review the 25 pages of changes. Dispensing with the usual practice of alternating between Majority and Minority amendments, after offering his own amendment, Chairman Sensenbrenner recognized, over Democratic protestations, Rep. Dan Lungren (R-CA) to offer an amendment that substantially altered the underlying bill. By virtue of its scope, the Majority's amendment precluded numerous additional Democratic amendments. Rep. Conyers raised a "point of procedure," recalling that the normal practice is to alternate between Majority and Minority Members. Chairman Sensenbrenner responded by saying "Well, the Gentleman from California is very pushy so he's been recognized."²⁹ It is also notable and unfortunate that the

²⁵Letter from Glenn A. Fine, Inspector General, Department of Justice, to Congresswoman Zoe Lofgren *et. al.* (Jan. 4, 2006); Letter from Thomas F. Gimble, Acting Inspector General, Department of Defense, to Congresswoman Zoe Lofgren *et. al.* (Jan. 10, 2006).

²⁶Dan Eggen, *Bush Thwarted Probe into NSA Wiretapping*, WASH. POST, July 19, 2006, at A4 (referring to testimony of Attorney General Alberto Gonzales before the Senate Judiciary Committee).

²⁷H. Res. 819, 109th Cong., 2d Sess.

²⁸Letters from Democratic Members, U.S. House Comm. on the Judiciary, to Robert Deitz, General Counsel, NSA (Sept. 12, 2006).

²⁹*Markup of H.R. 5825, the "Electronic Surveillance Modernization Act," House Comm. on the Judiciary*, 109th Cong., 2d Sess. (Sept. 20, 2006). Once debate began on the amendment, Representative Conyers asked that the amendment be withdrawn until the Members had time to digest its contents. Mr. Conyers acknowledged the possibility that Democrats might agree with the substance of the amendment but that more time was needed to review it. He also noted that there were changes to at least 6 sections of the underlying bill, that the amendment was 25 pages long, and that staff for the Minority had not been consulted about any of these

Chairman ruled Rep. Cannon's amendment which provided that notwithstanding any other law precludes court review of "any alleged intelligence program involving electronic surveillance" to be in order, again over Democratic objections. In point of fact, such an amendment falls outside the jurisdiction of the Judiciary Committee's jurisdiction should not have been considered at our markup.

Conclusion

We believe that every communication to and from an al Qaeda member should be subject to government surveillance and support Congress providing the President with the tools needed to accomplish that goal. In doing so, however, Congress must not abdicate its responsibility or negate the role of the courts to act as a check against unilateral presidential powers. We dissent from the legislation before us because it fails to rein in the president's warrantless surveillance program, expands the NSA's authority to expose millions of innocent Americans to warrantless surveillance, jeopardizes the privacy rights of American citizens and raises serious and significant constitutional concerns. The American people deserve better than this bill and this ill-conceived process of legislating.

John Conyers, Jr.
Howard L. Berman
Rick Boucher
Jerrold Nadler
Robert C. Scott
Melvin L. Watt
Zoe Lofgren
Sheila Jackson Lee
Maxine Waters
Martin T. Meehan

William D. Delahunt
Robert Wexler
Anthony D. Weiner
Adam B. Schiff
Linda T. Sanchez
Chris Van Hollen
Debbie Wasserman Schultz

changes. He stated that it was "impossible for this Member to gain any appreciation of the significant changes the Gentleman has attempted" and asked that it be withheld until Democrats had the "opportunity to examine it with the care that is required." *Id.* Representative Schiff also asked for cooperation in light of the fact that he and Representative Flake had been working on a bipartisan substitute to the underlying bill. He noted that there was no way to know how the changes from the Lungren amendment affected the carefully drafted substitute. *Id.* Representative Conyers moved to table the Lungren amendment but the Chairman prohibited the motion from being offered. Representative Nadler then moved to adjourn the Committee meeting until the following day so that the Members could have a chance to review the amendment. On a party-line vote, this motion was defeated 14-17. The amendment eventually passed the committee by a vote of 17-2.